REMARKS

The Office Action mailed August 31, 2007 has been reviewed and the comments of the Patent and Trademark Office have been considered. Claims 1-14 were pending in the application. Claims 1, 3, 4, 6, 7 and 13 have been amended. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, are presented, with an appropriate defined status identifier. Thus, claims 1-14 remain pending in the application.

Prior Art Rejections

Claims 1-9 and 13 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 7,039,803 to Lotspiech (hereinafter "Lotspiech") in view of U.S. Patent Application Publication 2002/0029337 to Sudia (hereinafter "Sudia"). Claims 10-12 and 14 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Sudia in view of Lotspiech. Applicant respectfully traverses these rejections for at least the following reasons.

The independent claims recite several features that are not found in either Lotspiech or Sudia. Independent claim 1 recites "allocating within the hierarchy a distinct subtree for each group of users," and "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping." Independent claim 10 recites "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled." Independent claims 13 and 14 recite analogous features. The invention as claimed issues keys to user based upon the group (or level of service) to which they are associated. Thus, there is an association between the user and an outside entity, which is utilized to assign or allocate keys to the user. There is no teaching or suggestion of such a feature in either Lotspiech or Sudia.

The Examiner relies on Lotspiech to teach this feature. Specifically, the Examiner cites Lotspiech's teaching:

> "A method is disclosed for grouping users into (possibly overlapping) subsets of users, each subset having a unique, preferably long-lived subset key, and **assigning each user respective private information I_u**. The

method also includes selecting at least one preferably short-lived session encryption key K, and **partitioning users not in a revoked set R into disjoint subsets $S_{i1}, \ldots S_{im}$ having associated subset keys $L_{i1}, \ldots, L_{im}$.** The session key K is encrypted with the subset keys $L_{i1}, \ldots, L_{im}$ to render m encrypted versions of the session key K. In one aspect, **the users can establish leaves in a tree such as a complete binary tree, and the subsets $S_{i1}, \ldots S_{im}$ are induced by the tree.**" (column 3, lines 11-23)

Thus, users are assigned private information I_u that is used for decrypting the subset keys. However, there is no teaching or indication in this passage that users are assigned keys based upon the group in which they are in, or the level of service provision with which they are associated. In Lotspiech, the users are partitioned into disjoint subsets that have associated subset keys, but there is no indication that the users are assigned keys. Rather, the users are assigned private information that is utilized to decrypt the subset keys (column 6, lines 41-53).

This private information is obtained from the labels of nodes that are not in direct path between the receiver and the root node. Thus, if the user was grouped in a certain group, which was in a specific subtree of the hierarchical tree, the labels would be obtained from an ancestor of the receiver node. Thus, the labels utilized to make the private information that is assigned to the user is not derived from associations of the user, but rather from nodes that are explicitly NOT associated with the user. Further, in independent claims 1 and 13, the keys are issued from the subtree associated with a distinct group in which the user resides. There is no indication in Lotspiech that the labels are obtained from the subtree in which the receiver resides based upon its grouping. Rather, Lotspiech seemingly teaches the opposite – that the labels would be obtained by nodes "that 'hang' off the direct path and are inducted by some node vi, and ancestor of u." (column 10, lines 3-10) Thus, Lotspiech clearly fails to teach "allocating within the hierarchy a distinct subtree for each group of users," and "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping." Correspondingly, Lotspiech also fails to teach "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled." As shown above, there is no indication or teaching in Lotspiech of allocating a key to a user based upon the associations of that user. Thus, Lotspiech fails to teach all of the features of the independent claims.

Sudia fails to overcome the deficiencies of Lotspiech as detailed above. First of all, Sudia does not even describe a hierarchy of certificates, from which two groups of users could be obtained. Rather, Sudia teaches the well-known hierarchical structure of the X.500 directory model and asserts that the way that attributes are specified **in** a certificate can follow the X.500 model (paragraphs 0046-0050). Sudia explicitly states that "Because many authorization decisions are based on the user's position in an organization, the organizational structure and the user's position therein may be specified as part of a user's name." (paragraph 0047) That is, Sudia is here teaching that the user's name in a certificate can reflect their position in the organization. Sudia provides support for this teaching by further stating that "[N]ames in certificates are specified in terms of the X.500 Directory model, as follows." (paragraph 0047)

Sudia also states: "Several of the attributes defined in X.500 may be usefully included *in the user's attribute certificate*. For example, the object class can be used to distinguish between entities (for example users and roles) whose distinguished names are of the same form." (paragraph 0050)

> "In addition to the use of the DIT to group entities along organizational lines, X.500 defines several object classes that can be used to construct arbitrary groups of entities." (paragraph 0051) This is simply saying that an arbitrary group can be defined upon the basis of the value of a particular certificate attribute. Thus a certificate may have a role attribute which may have a value such as "uspto examiner."

The passage in Sudia referred to by the examiner therefore does not disclose a hierarchy of certificates but simply how the user name attribute of a certificate can indicate the user's position in an organisation in a manner similar to that used in a X.500 directory. Thus, Applicants again respectfully submit that the combination of Sudia with Lotspiech would not teach the invention as claimed and would not be a valid combination in terms of combining the two technologies. There would not be a reasonable expectation of success in joining the teachings of Sudia with those of Lotspiech.

Even if this combination were to be incorrectly made, there is no mention in Sudia of assigning or allocating keys to a user based upon their associations. Sudia teaches assigning users public or secret keys, as are well-known in the art of cryptography. (paragraphs 0006-0010) There is no teaching or suggestion in Sudia of assigning or allocating a key to a user based upon the user's associations. Sudia does teach augmenting a certificate with information about the user (such as role, organization, etc.) as detailed above, but there is no teaching or suggestion that this user information is utilized in assigning the user a key. In fact, Sudia teaches that:

> "One likely approach to creating this device certificate would be to generate the device key pair during fabrication of the smartcard so that the corresponding device certificate 1302 could also be included on the card. The device certificate 1302 certifies the properties 1304 of the card, and the card generates a key pair 1303,1309 which is to be used by the user of the card and which the user can have certified as his own by any appropriate desired CA." (paragraph 0111).

Thus, Sudia also fails to teach all of the features of the invention as claimed, specifically failing to teach both "allocating within the hierarchy a distinct subtree for each group of users" and "issuing keys to users from subtrees within the hierarchy upon the basis of their grouping," and "allocating keys to users which are indicative to a service provider of the level of service to which they are entitled." Thus, if this rejection is maintained, the Examiner is respectfully requested to point out where these features are found in either Lotspiech or Sudia.

The dependent claims that depend from the independent claims are also patentable for at least the same reasons as the independent claims on which they ultimately depend. In addition, they recite additional patentable features when considered as a whole.

Conclusion:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 C.F.R. § 1.25. Additionally, charge any fees to Deposit Account 08-2025 under 37 C.F.R. § 1.16 through § 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees.

Respectfully submitted,

By (Reg. 59597)

for/ William T. Ellis
Attorney for Applicant
Registration No. 26,874

Date: October 26, 2007

HEWLETT PACKARD
Customer Number: 22879
Telephone: (202) 672-5485
Facsimile: (202) 672-5399